(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication : **0 171 323**
B1

(12) # FASCICULE DE BREVET EUROPÉEN

(45) Date de publication du fascicule du brevet : **07.09.88**

(51) Int. Cl.⁴ : **E 05 B 49/00**, G 07 C 9/00

(21) Numéro de dépôt : **85401476.8**

(22) Date de dépôt : **18.07.85**

(54) **Installation de commande et de contrôle des différentes serrures codées d'un ensemble.**

(30) Priorité : **18.07.84 FR 8411399**

(43) Date de publication de la demande :
12.02.86 Bulletin 86/07

(45) Mention de la délivrance du brevet :
07.09.88 Bulletin 88/36

(84) Etats contractants désignés :
DE GB IT

(56) Documents cités :
EP-A- 0 043 270
EP-A- 0 044 630
EP-A- 0 098 437
GB-A- 2 118 614
GB-A- 2 124 808

(73) Titulaire : **Lewiner, Jacques**
5, rue Bory d'Arnex
F-92210 Saint-Cloud (FR)

Hennion, Claude
18, rue Flatters
F-75005 Paris (FR)

(72) Inventeur : **Lewiner, Jacques**
5, rue Bory d'Arnex
F-92210 Saint-Cloud (FR)
Inventeur : **Hennion, Claude**
18, rue Flatters
F-75005 Paris (FR)

(74) Mandataire : **Behaghel, Pierre et al**
CABINET PLASSERAUD 84 rue d'Amsterdam
F-75009 Paris (FR)

EP 0 171 323 B1

Description

L'invention concerne les installations de commande et de contrôle des différentes serrures codées d'un ensemble comportant un nombre relativement élevé de telles serrures, ce nombre étant de préférence supérieur à 50 et même à 100.

Elle concerne plus particulièrement, parce que c'est dans leur cas que son application semble devoir offrir le plus d'intérêt, mais non exclusivement, parmi ces installations, celles équipant les hôtels comprenant un grand nombre de chambres, chacune de ces chambres étant accessible par une porte équipée d'une serrure codée, laquelle serrure est commandable électriquement à l'aide d'une clé codée en correspondance.

Les clés codées en question sont de préférence des cartes portant un code enregistré sous forme magnétique ou optique, ou encore des émetteurs portables de codes se présentant sous la forme d'ondes électromagnétiques ou ultrasonores, et les codes considérés sont des nombres exprimés par des suites de signaux binaires.

Les clés codées peuvent être également constituées par un code immatériel confié de façon intelligible à un usager habilité, par exemple sous la forme d'une suite de chiffres et/ou de lettres, et destiné à être composé sur un clavier disposé à proximité de la serrure ou à être reproduit de toute autre manière désirable.

Dans les installations du genre indiqué, les personnes habilitées au déverrouillage d'une serrure donnée ne le sont que provisoirement et changent fréquemment.

Il faut donc éviter qu'un utilisateur mal intentionné puisse continuer à déverrouiller la serrure considérée au-delà de l'expiration de la période au cours de laquelle il en détenait l'autorisation, et ce à l'aide d'une copie de la clé qui lui avait été confiée alors ou à l'aide de cette clé elle-même, conservée par lui au-delà de ladite expiration.

Pour obtenir un tel résultat, il a déjà été proposé d'invalider automatiquement la clé affectée à chaque serrure par simple présentation à cette serrure d'une nouvelle clé détenue par l'utilisateur habilité suivant.

Dans certains modes de réalisation connus des installations conçues à cet effet, le code attribué à chaque clé par un émetteur central de clés comporte deux portions enregistrées respectivement sur deux plages distinctes de la clé, savoir une première portion affectée directement au déverrouillage de la serrure et une seconde portion affectée au changement de code.

Pour simplifier, on appellera ci-après « première clé » une clé confiée à un premier utilisateur habilité au déverrouillage d'une serrure donnée et « seconde clé » une clé confiée ultérieurement à un second utilisateur que l'on désire habiliter à son tour en supprimant l'habilitation du premier, et on désignera respectivement par A et B les portions de code enregistrées par l'émetteur central de clés sur les deux plages de la première clé et par B' et C les portions de code enregistrées respectivement sur les deux plages de la seconde clé.

Dans les modes de réalisation connus, les codes B et B' sont identiques.

La serrure concernée comprend à l'origine des moyens pour asservir son déverrouillage à la lecture du code partiel A sur la première plage d'une clé, des moyens pour mettre en mémoire le code partiel B porté sur la seconde plage d'une telle clé portant le code partiel A sur sa première plage, et des moyens de comparaison.

Tant que la première clé correcte est présentée à la serrure, la lecture du code partiel A de sa première plage assure directement le déverrouillage de cette serrure et le code partiel B n'intervient que par sa mise en mémoire.

Lors de la présentation de la seconde clé, la section de déverrouillage de la serrure ne lit plus le code partiel correct A sur la première plage de cette clé, mais le code partiel B.

C'est alors qu'interviennent les moyens de comparaison de la serrure : ceux-ci comparent le code partiel (ici B) mis en mémoire précédemment en provenance de la seconde plage de la première clé au nouveau code partiel lu sur la première plage de la seconde clé.

L'identification résultant d'une telle comparaison a pour effet de déverrouiller la serrure, de faire adopter par cette serrure le code ainsi identifié, c'est-à-dire ici le code partiel B, comme nouveau code de déverrouillage et d'invalider, par effacement ou autrement, le code partiel A de déverrouillage initial.

C'est alors le code partiel C de la seconde plage de la seconde clé qui assure le rôle du code partiel B précédent, et ainsi de suite.

Une telle formule — qui a fait notamment l'objet des brevets US n° 3 821 704, n° 3 860 911, n° 4 207 555 et n° 4 213 118 — présente l'important avantage de permettre une invalidation automatique des clés périmées par la simple utilisation ultérieure des clés valides sans qu'il soit nécessaire de procéder à d'autres interventions locales.

Mais elle n'est pas à l'abri des fraudes.

En effet, il est relativement facile pour un utilisateur mal intentionné qui réussit à se faire confier deux clés d'habilitation successives affectées à une même serrure de détecter par comparaison entre les codes enregistrés sur ces deux clés le code partiel commun à celles-ci, savoir B dans l'exemple ci-dessus, et donc d'en déduire le code partiel de déverrouillage (ici C) de la clé suivante de la série correspondant à la serrure considérée et d'établir lui-même une telle clé suivante à l'insu et à la place de l'émetteur central de clés.

Cette clé suivante, bien que « faussement » émise, permet de déverrouiller la serrure considérée aussi bien que la « vraie » clé suivante.

Pour bénéficier de l'avantage signalé ci-dessus tout en rendant impossible la fraude qui vient d'être indiquée, il a été proposé, par exemple

dans la demande EP-A-0043270, une installation de commande et de contrôle comprenant encore, comme précédemment, un émetteur propre à élaborer des clés codées de commande de serrures et un lecteur associé à chaque serrure, propre à déverrouiller cette serrure sur simple présentation à celui-ci d'une clé codée correctement, cet émetteur et ce lecteur étant agencés de façon telle que la détection par ledit lecteur du code y enregistré par ledit émetteur sur chaque nouvelle clé d'ordre p affectée à la serrure associée à ce lecteur se traduise par l'invalidation du code x enregistré sur la clé d'ordre p — 1 précédemment affectée à cette serrure, de rendre chaque code y déductible du code x par un algorithme $y = f(x)$ mis en mémoire au moins dans l'émetteur.

Par « algorithme » on entend dans le présent texte un ensemble d'opérations numériques faisant correspondre à un premier nombre x un second nombre y.

Chacun des appareils émetteur et lecteur est alors équipé de façon à exploiter l'algorithme de manière appropriée.

C'est ainsi que l'émetteur élaborant les clés successives destinées à déverrouiller à tour de rôle la serrure équipée du lecteur considéré est agencé de façon à enregistrer respectivement sur ces clés successives les codes x, $f(x)$, $f^2(x)$ ... $f^n(x)$...

Dans l'alinéa précédent, n désigne un entier, $f^n(x)$ signifie $f[f^{n-1}(x)]$ et le symbole $f(x)$ est équivalent à $f^1(x)$.

Quant au lecteur associé à la serrure considérée, il est agencé de façon à comparer successivement les codes lus sur les différentes clés avec les codes x, $f(x)$, $f^2(x)$, ..., $f^n(x)$... et à déverrouiller la serrure quand la comparaison effectuée révèle une identité.

En outre le lecteur est équipé de moyens pour invalider automatiquement chaque code $f^p(x)$ lorsque la clé portant le code $f^{p+1}(x)$ lui est présentée.

Dans ces conditions, chaque sous-ensemble lecteur-serrure est agencé de façon telle qu'à un instant donné la serrure puisse être déverrouillée par la présentation au lecteur de l'un ou l'autre de deux codes $f^p(x)$ et $f^{p+1}(x)$, la présentation du premier de ces deux codes se traduisant par le déverrouillage seul de la serrure alors que la présentation du second code se traduit non seulement par ce déverrouillage, mais aussi par l'invalidation du premier code et par la sensibilisation du lecteur au code suivant $f^{p+2}(x)$ de la série, les rôles joués respectivement juste avant cette présentation du second code $f^{p+1}(x)$ par les deux premiers codes étant joués respectivement à partir de cet instant par les deux codes $f^{p+1}(x)$ et $f^{p+2}(x)$.

Dans les modes de réalisation connus d'une telle installation, chaque lecteur n'est sensible à chaque instant qu'à deux codes, savoir les codes $f^p(x)$ et $f^{p+1}(x)$ dans l'exemple ci-dessus.

Une telle formule exige une synchronisation rigoureuse entre l'émetteur et chaque lecteur.

Il peut arriver en effet qu'une « première clé » élaborée par l'émetteur à destination d'une serrure donnée ne soit pas utilisée effectivement avant l'élaboration de la clé suivante ou « seconde clé » par ledit émetteur.

Il résulte d'un tel défaut d'utilisation un défaut de progression dans la suite des codes lisibles par le lecteur associé à ladite serrure, ce qui rend inopérante ladite « seconde clé » pour l'ouverture de cette serrure.

Cet inconvénient est particulièrement manifeste lorsque chacune des clés considérées est habilitée à l'ouverture d'une pluralité de serrures : dans un tel cas, il peut arriver que l'une au moins desdites serrures n'ait pas été effectivement actionnée par la « première clé » correspondante au cours de la période d'habilitation de cette clé.

L'invention permet de remédier à cet inconvénient.

A cet effet chaque lecteur est rendu sensible à chaque instant à un nombre m supérieur à deux de codes non invalidés de la suite des codes $f^p(x)$, $f^{p+1}(x)$, $f^{p+2}(x)$... déductibles les uns des autres par l'algorithme $f(x)$.

Ce lecteur est alors agencé de façon telle qu'en lisant l'un quelconque des codes valides de cette suite, il invalide automatiquement tous les codes de rang inférieur de ladite suite.

Dans ces conditions, la serrure associée audit lecteur peut être ouverte à chaque instant par la dernière clé élaborée par l'émetteur à destination de cette serrure.

Le nombre m est choisi en fonction du risque réel présenté par le défaut signalé ci-dessus : il est de préférence compris entre 5 et 100, étant par exemple de l'ordre de 10.

Les différents codes de la suite considérée peuvent être enregistrés à l'avance dans une mémoire du lecteur concerné, le nombre de ces codes valides diminuant progressivement à raison des invalidations successives des clés.

Une telle solution présente certes l'avantage de rendre inutile l'exploitation locale réelle de l'algorithme $f(x)$, mais elle exige de recharger chroniquement la mémoire du lecteur.

Dans tous les cas le lecteur peut être équipé de moyens pour compter et enregistrer le nombre des changements de codes intervenus depuis l'origine de la vie de la serrure ou depuis un instant déterminé de remise à zéro.

Selon un mode de réalisation intéressant, l'algorithme $y = f(x)$ adopté pour tous les lecteurs est le même, mais le code de départ x, de la suite x, $f(x)$, $f^2(x)$..., $f^n(x)$..., qui est affecté initialement au déverrouillage de chaque serrure, diffère de ceux affectés initialement aux autres serrures.

Dans un tel cas, on peut enregistrer comme précédemment dans une mémoire de chaque lecteur la suite de codes adéquate : l'identification du premier code, de cette suite, valide à un instant donné peut alors être obtenue par le simple comptage, évoqué ci-dessus, du nombre des changements de codes intervenus depuis un instant de départ donné, qui peut être un instant de remise à zéro, comptage complété bien entendu par la connaissance du code de départ

affecté à la serrure concernée.

Cette solution simplifie également la construction de l'émetteur puisqu'elle fait appel à un seul algorithme en tout et pour tout pour l'établissement de la totalité des clés.

Cette simplification est très importante puisque, par exemple pour l'application de l'invention à la desserte d'un hôtel de 100 chambres, elle revient à diviser par 100 le nombre des algorithmes enregistrés dans l'émetteur ainsi que le nombre des circuits de calcul et de transformation correspondants.

La contrepartie de cette simplification — savoir la nécessité d'identifier correctement les différents codes de départ affectés aux différentes serrures et les nombres des changements de codes subséquents — ne supprime qu'une faible partie de l'avantage ainsi obtenu.

En suite de quoi, et quel que soit le mode de réalisation adopté, on dispose finalement d'une installation de commande et de contrôle des différentes serrures codées d'un ensemble, dont la constitution et le fonctionnement résultent suffisamment de ce qui précède.

Cette installation présente un certain nombre d'avantages par rapport à celles antérieurement connues.

En particulier, par rapport aux installations antérieures du premier type évoquées dans l'introduction,

— elle rend impossibles les fraudes signalées : en effet, l'utilisateur mal intentionné qui réussirait à se faire confier deux clés successivement habilitées au déverrouillage d'une serrure donnée peut certes en déduire les deux codes x et y enregistrés respectivement sur ces deux clés, mais il ne pourra pas en déduire l'algorithme f(x) qui relie ces deux codes car le nombre d'algorithmes reliant deux nombres entre eux est infini : il ne pourra donc pas élaborer « faussement » une clé suivante de la série concernée ;

— la richesse de chaque code de déverrouillage enregistré sur une clé donnée est très supérieure à celles des codes partiels desdites installations antérieures du fait que la plage disponible pour l'enregistrement de ce code sur chaque clé est deux fois plus grande.

Par rapport aux installations antérieures du second type évoquées dans l'introduction, l'installation ici proposée permet de s'affranchir des servitudes de la « synchronisation » entre l'émetteur et les lecteurs, les absences d'usage de certaines « premières clés » ne se traduisant plus ici par la neutralisation des « secondes clés » correspondantes.

Comme il va de soi, et comme il résulte d'ailleurs déjà de ce qui précède, l'invention ne se limite nullement à ceux de ses modes d'application et de réalisation qui ont été plus spécialement envisagés ; elle en embrasse, au contraire, toutes les variantes, notamment celles où l'algorithme permettant d'élaborer le code y à partir du code précédent x serait fonction non seulement de ce code précédent, mais également d'un numéro affecté à l'ensemble serrure-lecteur concerné, numéro enregistré à la fois dans cet ensemble et dans l'émetteur, notamment dans le cas où le nombre desdits ensembles serait particulièrement élevé.

Revendications

1. Installation de commande et de contrôle des différentes serrures codées d'un ensemble, comprenant : un émetteur propre à élaborer des clés codées de commande desdites serrures et un lecteur associé à chaque serrure, propre à déverrouiller cette serrure sur simple présentation à celui-ci d'une clé codée correctement, cet émetteur et ce lecteur étant agencés de façon telle que la détection par ledit lecteur du code y enregistré par ledit émetteur sur chaque nouvelle clé d'ordre p affectée à la serrure associée à ce lecteur se traduise par l'invalidation du code x enregistré sur la clé d'ordre p — 1 précédemment affectée à cette serrure, chaque code y étant déductible du code x par un algorithme $y = f(x)$ mis en mémoire au moins dans l'émetteur, caractérisée en ce qu'à chaque instant le lecteur est sensible simultanément à un nombre m supérieur à deux de codes non invalidés de la suite x, $f(x)$, $f^2(x)$..., $f^n(x)$, dans laquelle $f^n(x) = f[f^{n-1}(x)]$, et est agencé de façon telle qu'en lisant l'un quelconque de ces codes, il invalide automatiquement tous les codes de rang inférieur de la suite considérée.

2. Installation selon la revendication 1, caractérisée en ce que le nombre m est compris entre 5 et 100.

3. Installation selon l'une quelconque des précédentes revendications, caractérisée en ce que le lecteur est équipé de moyens pour compter et enregistrer le nombre des changements de codes intervenus depuis un instant de départ ou de remise à zéro.

4. Installation selon l'une quelconque des précédentes revendications, caractérisée en ce qu'un seul et même algorithme est adopté pour les différentes serrures, les codes affectés au déverrouillage de ces différentes serrures à chaque instant différant les uns des autres en raison des choix différents adoptés pour les codes de départ respectifs.

5. Installation selon l'une quelconque des précédentes revendications, caractérisée en ce que l'algorithme permettant d'élaborer le code y à partir du code précédent x est fonction non seulement de ce code précédent, mais également d'un numéro affecté à l'ensemble serrure-lecteur concerné, numéro enregistré à la fois dans cet ensemble et dans l'émetteur.

Claims

1. Installation for controlling and monitoring the different coded locks of an assembly, comprising : an emitter capable of elaborating coded keys for controlling said locks and a reader associated with each lock, for unlocking this lock

on simple presentation thereto of a correctly coded key, this emitter and this reader being adapted so that detection by said reader of the code y recorded by said emitter on each new key of order p assigned to the lock associated with this reader results in the invalidation of the code x recorded on the key of order p — 1 previously assigned to this lock, each code y being derived from code x by an algorithm $y = f(x)$ stored in at least the emitter, characterized in that at any time the reader is responsive simultaneously to a number m greater than 2 of non invalidated codes of the succession x, $f(x)$, $f^2(x)$..., $f^n(x)$, where $f^n(x) = f[f^{n-1}(x)]$, and is adapted so that by reading any one of these codes, it automatically invalidates all the lower rank codes of the succession considered.

2. Installation according to claim 1, characterized in that the number m is between 5 and 100.

3. Installation according to any one of the preceding claims, characterized in that the reader is equipped with means for counting and recording the number of code changes taking place from a starting or resetting time.

4. Installation according to any one of the preceding claims, characterized in that one and the same algorithm is adopted for the different locks, the codes assigned to the unlocking of these different locks at any time differing from each other because of the different choices adopted for the respective starting codes.

5. Installation according to any one of the preceding claims, characterized in that the algorithm for elaborating the code y from the preceding code x is a function not only of this preceding code, but also of a number assigned to the lock-reader assembly concerned, which number is recorded both in this assembly and in the emitter.

Patentansprüche

1. Einrichtung zum Betreiben und Kontrollieren von einer mit unterschiedlichen Kombinationsschlössern versehenen Anlage, die aufweist: einen Sender, der geeignet ist, das Betreiben der Schlösser mit Kombinationsschlüsseln auszufüllen, und eine Abtasteinrichtung, die jedem Schloss zugeordnet ist und die dieses Schloss einfach entriegeln kann, wenn ein richtiger Kombinationsschlüssel zu ihm zugewiesen wird, wobei der Sender und die Abtasteinrichtung derart betreibbar sind, dass die Detektion durch die Abtasteinrichtung der vom Sender gespeicherten Kombination y auf jedem neuen Schlüssel der Ordnung p, der an dem Abtasteinrichtung zugeordneten Schloss zugewiesen ist, durch die Löschung der Kombination x, die für den Schlüssel der Ordnung p — 1 gespeichert ist, übersetzt wird, welcher Schlüssel vorangehend für dieses Schloss genommen wurde, wobei jede Kombination y von der Kombination x durch einen Algorithmus $y = f(x)$ ableitbar ist, der wenigstens im Sender gespeichert ist, dadurch gekennzeichnet, dass jedesmal die Abtasteinrichtung gleichzeitig eine Zahl m grösser als zwei von nichtgelöschten Kombinationen der Folge x, $f(x)$, $f^2(x)$..., $f^n(x)$ empfängt, wobei $f^n(x) = f[f^{n-1}(x)]$ ist und derart betrieben wird, dass wenn irgendeine der Kombinationen gelesen wird, automatisch alle Kombinationen der niederen Rangordnungen der betreffenden Folge gelöscht werden.

2. Einrichtung nach Anspruch 1, dadurch gekennzeichnet, dass die Zahl m zwischen 5 und 100 ist.

3. Einrichtung nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die Abtasteinrichtung mit Einrichtungen versehen ist, um die Anzahl der Änderungen der Kombinationen, ausgehend von einem Anfangszeitpunkt oder einer Rückstellung auf Null, zu zuzählen und zu speichern.

4. Einrichtung nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass ein und derselbe Algorithmus für die unterschiedlichen Schlösser verwendet wird, und dass die eine Entriegelung der unterschiedlichen Schlösser zu jedem Zeitpunkt bewirkenden Kombinationen sich voneinander aufgrund von unterschiedlichen Wahlmöglichkeiten unterscheiden, die für die jeweiligen Ausgangskombinationen angenommen werden.

5. Einrichtung nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass der Algorithmus, der die Verarbeitung der Kombination y, ausgehend von der vorangehenden Kombination x, ermöglicht, eine Funktion nicht nur dieser vorangehenden Kombination, sondern auch von einer Zahl ist, die einer betreffenden Schloss-Abtasteinrichtungsanlage zugewiesen ist, wobei diese Zahl gleichzeitig in dieser Anlage und im Sender gespeichert ist.